JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

DHRUV THUKRAL, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Los Angeles Cnty., CA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

DEFENDANTS

HEALTHEQUITY, INC., WAGEWORKS, INC., and FURTHER OPERATIONS, LLC

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)

Brief description of cause:
Unauthorized disclosure of Plaintiff and Class Members' personal information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Hon. Jill N. Parrish DOCKET NUMBER 2:24-cv-00528-JNP

DATE
August 6, 2024

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

Jared Scott
Jake W. Nelson
jscott@aklawfirm.com
jnelson@aklawfirm.com
ANDERSON & KARRENBERG
50 West Broadway, Suit 600
Salt Lake City, UT 84101
Telephone: 801.534.1700
Facsimile: 801.364.7697

Attorneys for Plaintiff and the Proposed Classes

Andrew W. Ferich*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585
**Pro hac vice* to be filed

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, CENTRAL DIVISION

DHRUV THUKRAL, individually and on behalf of all others similarly situated, Plaintiff, v. HEALTHEQUITY, INC., WAGEWORKS, INC., and FURTHER OPERATIONS, LLC, Defendants.	**COMPLAINT** **[PROPOSED CLASS ACTION]** **JURY TRIAL DEMANDED** Case No.

Plaintiff Dhruv Thukral ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class Members"), by and through his attorneys, brings this Class Action Complaint against Defendants HealthEquity, Inc., WageWorks, Inc. ("WageWorks"), and Further Operations, LLC ("Further Operations") (collectively, "Defendants"), and complains and alleges upon personal knowledge as to himself and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard his and approximately 4,300,000 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including first name, last name, address, telephone number, employee ID, employer, Social Security number, health card number, health plan member number, dependent information, HealthEquity benefit type, diagnoses, prescription details, payment card information, and HealthEquity account type.

2. HealthEquity, WageWorks, and Further Operations are companies that manage health savings accounts and other consumer-directed benefits. HealthEquity is the parent company of WageWorks and Further Operations.

3. On or about March 25, 2024, HealthEquity discovered that an unauthorized third party had gained access to its network systems and obtained files containing the PII/PHI of Defendants' customers (the "Data Breach").

4. Defendants owed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their customers' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class Members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII/PHI was exposed as a result of the Data Breach, which Defendants discovered on or about March 25, 2024.

6. Plaintiff, on behalf of himself and all other Class Members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, violations of the California Consumer Privacy Act, and violations of the California Customer Records Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Dhruv Thukral

7. Plaintiff Dhruv Thukral is a citizen of California.

8. Defendants manage Plaintiff Thukral's health savings account. As a condition of providing such services, Defendants required Plaintiff Thukral to provide them with his PII/PHI.

9. Plaintiff Thukral believed Defendants had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff Thukral provided his PII/PHI to Defendants in connection with receiving its services.

10. At all relevant times, Defendants stored and maintained Plaintiff Thukral's PII/PHI on its network systems.

11. Plaintiff Thukral takes great care to protect his PII/PHI. Had Plaintiff Thukral known that Defendants do not adequately protect the PII/PHI in its possession, he would not have utilized Defendants' services or otherwise agreed to entrust Defendants with his PII/PHI.

12. As a direct result of the Data Breach, Plaintiff Thukral has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

Defendant HealthEquity, Inc.

13. Defendant HealthEquity, Inc. is a Delaware corporation with its principal place of business located at 15 W. Scenic Pointe Drive, Suite 100, Draper, Utah 84020. It may be served through its registered agent: C T Corporation System, 1108 E. South Union Ave., Midvale, Utah 84047.

Defendant WageWorks, Inc.

14. Defendant WageWorks, Inc. is a Delaware corporation with its principal place of business located at 15 W. Scenic Pointe Drive, Suite 100, Draper, Utah 84020. It may be served through its registered agent: C T Corporation System, 1108 E. South Union Avenue, Midvale, Utah 84047.

Defendant Further Operations, LLC

15. Defendant Further Operations, LLC is a Delaware limited liability company with its principal place of business located at 15 W. Scenic Pointe Drive, Suite 100, Draper, Utah 84020. It may be served through its registered agent: C T Corporation System, 1108 E. South Union Avenue, Midvale, Utah 84047

JURISDICTION AND VENUE

16. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

17. This Court has general personal jurisdiction over Defendants because they maintain their principal places of business in this State, regularly conduct business in this State, contract to supply services or goods in this State, and have sufficient minimum contacts in this State.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' principal places of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

19. HealthEquity is "a leader and an innovator in providing technology-enabled services that empower consumers to make healthcare saving and spending decisions."[1] HealthEquity is a company that manages health savings accounts and other consumer-directed benefits, including flexible spending accounts, health reimbursement arrangements, and other benefits.[2] HealthEquity also offers an investment platform and advisory service.[3]

20. WageWorks and Further Operations are also companies that administer health savings accounts and other consumer-directed benefits.[4] WageWorks and Further Operations are wholly owned subsidiaries of HealthEquity.[5]

21. In the regular course of its business, Defendants collect and maintain the PII/PHI of their current and former customers. Defendants required Plaintiff and Class Members to provide their PII/PHI as a condition of receiving services from Defendants.

---

[1] *Form 10-K*, HEALTHEQUITY (Mar. 22, 2024), https://ir.healthequity.com/node/13391/html#i87f8de57eee54ba9829529ac9c466718_157.
[2] *Id.*
[3] *Id.*
[4] *See HealthEquity to Acquire WageWorks Accelerating Market-Wide Transition to HSAs*, HEALTHEQUITY (June 27, 2019), https://ir.healthequity.com/news-releases/news-release-details/healthequity-acquire-wageworks-accelerating-market-wide; *Product*, FURTHER, https://hellofurther.com/products/ (last accessed Aug. 1, 2024).
[5] *Form 10-K*, *supra* note 1.

22. HealthEquity promises it is committed to protecting the confidentiality, integrity, and availability of its customers PII/PHI, as well as its systems and applications. HealthEquity represents to its customers (including Plaintiff and Class Members) that it will employ secure design and testing practices and develop a world-class security and IT organization.

23. HealthEquity promises it takes numerous measures to promote cybersecurity and the protection of its customers' information, including investing in relevant tools and training for its employees and adopting a "Zero Trust" security approach that strengthens security by verifying who can access HealthEquity's systems.

24. HealthEquity represents it works with security architects and cybersecurity engineers to deploy controls designed to prevent or limit a cyberattack. HealthEquity further represents that it designs it products and services with privacy and transparency at the forefront.

25. HealthEquity claims to employ specific cybersecurity measures including, but not limited to: providing mandatory compliance, privacy, and security training to all persons with access to HealthEquity systems, an intrusion prevention program, third-party validation testing, and vulnerability testing.

26. In its Privacy Notice (the "Privacy Policy"), HealthEquity[6] claims its customers' privacy is important, and that it places a high priority on protecting customers' personal information. It also represents that it maintains administrative, technical, and physical safeguards to protect customers' PII/PHI from unauthorized access or acquisition.

[6] Upon information and belief, the terms of HealthEquity's Privacy Policy also apply to WageWorks and Further Operations.

27. HealthEquity admits in its Privacy Policy that it collects information subject to the requirements of HIPAA. HealthEquity claims it will honor all privacy rights defined by law, as stated in its Privacy Policy, and in applicable regulations.

28. The Privacy Policy describes the ways HealthEquity will use or share the PII/PHI it collects, including for delivering its services to its customers; detecting and preventing security incidents or illegal activity; or in accordance with customer's authorization or instructions.

29. HealthEquity promises it will only share its customers' PII/PHI as allowed in the Privacy Policy. It further promises it will limit access to customers' PII/PHI to only those people who need access to perform their duties.

30. In addition to the Privacy Policy, Further Operations also has a Notice of Privacy Practices (the "Privacy Notice") which describes the information it collects and how it uses that information and how PII/PHI will be used and disclosed, including for providing treatment and to receive and process payments.

31. In the Privacy Notice, Further Operations claims it has always been committed to maintaining the security and confidentiality of its customers' information. It represents that it maintains policies, procedures, and electronic controls to guard against the unauthorized access and use of its customers' PII/PHI.

32. Further Operations states it is responsible for implementing and enforcing policies and procedures to protect its customers' PII/PHI. Further Operations promises it takes every effort to comply with all federal and state privacy laws, including physical, electronic, and procedural measures.

33. Further Operations' Privacy Policy states its customers have the right to receive notification of data breaches of PII/PHI.

34. Plaintiff and Class Members are current or former customers of Defendants who entrusted Defendants with their PII/PHI.

The Data Breach

35. On or about March 25, 2024, HealthEquity "became aware of a systems anomaly" which it determined after an investigation resulted in "unauthorized access to or disclosure of protected health information and/or personally identifiable information stored in an unstructured data repository" on HealthEquity's systems.[7] The information disclosed in the Data Breach included the PII/PHI of Defendants' customers.[8]

36. The cybercriminals responsible for the Data Breach accessed and removed files containing the PII/PHI of Plaintiff and Class Members, including "first name, last name, address, telephone number, employee ID, employer, social security number, health card number, health plan member number, dependent information (for general contact information only), HealthEquity benefit type, diagnoses, prescription details, and payment card information (but not payment card number), and / or HealthEquity account type."[9]

37. While Defendants learned of the Data Breach on or about March 25, 2024, they waited until approximately August, 2024—over over four months later—to begin notifying their customers that their PII/PHI was in the hands of cybercriminals.[10]

---

[7] *Notice of Data Breach*, HEALTHEQUITY, https://www.healthequity.com/breach (last accessed Aug. 6, 2024).
[8] *Id.*; *see also Data Breach Notification Letter*, HEALTHEQUITY, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2ec3e314-5731-49d0-a937-6dc22c6b24f3.html; then click on the "Individual_Member_Notification_Non_HIPAA_exemplar.pdf" hyperlink.
[9] *See Notice of Data Breach*, *supra* note 7.
[10] *See Data Breach Noticiation*, ME. ATT'Y GEN. (July 26, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2ec3e314-5731-49d0-a937-6dc22c6b24f3.html.

38. Defendants' failure to promptly notify Plaintiff and Class Members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class Members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class Members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PII/PHI

39. At all relevant times, Defendants knew, or should have known, that the PII/PHI that it collected and stored was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII/PHI from cyberattacks that it should have anticipated and guarded against.

40. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[11]

41. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient records exposed.[12] This is an

[11] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[12] *See 2024 Breach Barometer*, PROTENUS 2, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-

increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[13]

42. PII/PHI is a valuable property right.[14] The value of PII/PHI as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

43. As a result of the real and significant value of these data, identity thieves and other cybercriminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last accessed June 28, 2024).

[13] *See id*.

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015) https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data, ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]").

[15] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last accessed Aug. 6, 2024).

[17] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

44. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[18] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[19]

45. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[20] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[21]

46. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[22] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[23]

---

[18] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[19] *Id.*
[20] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[21] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[22] Steager, *supra* note 18.
[23] *Id.*

47. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the figure is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[24]

48. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

49. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[25] [26]

50. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying

[24] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[25] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Aug. 6, 2024).

[26] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[27]

51. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[28]

52. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[29] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[30] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [31] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[32]

---

[27] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[28] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Aug. 6, 2024).

[29] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[30] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 21.

[31] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Aug. 6, 2024).

[32] *Id*.

53. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their healthcare records, most often the addition of falsified information through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [33]

54. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[34]

[33] *See* Dixon and Emerson, *supra* note 29.
[34] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

55. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and Class Members

56. Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI, which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

57. Plaintiff brings this action on behalf of himself and all members of the following classes (together, the "Class"):

> **Nationwide Class**
> All United States residents whose PII/PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.
>
> **California Class**
> All California residents whose PII/PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

58. Excluded from the Class are Defendants, their affiliates, parents, subsidiaries, employees, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge.

59. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

60. The members in the Class are so numerous that joinder of each of the Class Members in a single proceeding would be impracticable. HealthEquity reported to the Maine Attorney General's Office that the Data Breach impacted approximately 4,300,000 individuals.[35]

61. Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had a duty not to disclose the PII/PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

d. Whether an implied contract existed between Plaintiff and Class Members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;

e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class Members;

f. Whether Defendants breached their duties to protect Plaintiff's and Class Members' PII/PHI; and

[35] *Data Breach Notification*, *supra* note 8.

g. Whether Plaintiff and Class Members are entitled to damages and the measure of such damages and relief.

62. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

63. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

64. Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

65. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class Members to individually seek redress from Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation

creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

67. Plaintiff brings this claim on behalf of the nationwide class or, alternatively, on behalf of the California class based upon the laws of that state.

68. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding and protecting the PII/PHI in its possession, custody, or control.

69. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class Members' PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches in recent years targeting healthcare entities that collect and store PII/PHI.

70. Given the nature of Defendants' business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

71. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security

processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class Members' PII/PHI.

72. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII/PHI to unauthorized individuals.

73. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII/PHI would not have been compromised.

74. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI, which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Classes)

75. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

76. Plaintiff brings this claim on behalf of the nationwide class or, alternatively, on behalf of the California class based upon the laws of that state.

77. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

78. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure PII/PHI.

79. Defendants further have duties to Plaintiff under the California's Confidentiality of Medical Information Act ("CMIA") to maintain, store, and dispose of Plaintiff's and California Class Members' Medical Information in a manner that preserves its confidentiality.

80. Defendants violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the CMIA, by failing to, or contracting with companies that failed to, use reasonable measures to protect Plaintiff's and other Class Members' PII/PHI, by failing to provide timely notice, and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and

the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

81. Defendants' violations of HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the CMIA, constitutes negligence per se.

82. Plaintiff and Class Members are within the class of persons that HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the CMIA were intended to protect.

83. The harm occurring as a result of the Data Breach is the type of harm that HIPAA Privacy and Security Rules, and Section 5 of the FTCA, were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class Members as a result of the Data Breach.

84. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII/PHI to unauthorized individuals.

85. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the CMIA. Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses

associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI, which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Classes)

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

87. Plaintiff brings this claim on behalf of the nationwide class or, alternatively, on behalf of the California class based upon the laws of that state.

88. Plaintiff and Class Members gave Defendants their PII/PHI in confidence, believing that Defendants would protect that information. Plaintiff and Class Members would not have provided Defendants with this information had they known they would not be adequately protected. Defendants' acceptance and storage of Plaintiff's and Class Members' PII/PHI created a fiduciary relationship between the Defendants and Plaintiff and Class Members. In light of this relationship, Defendants must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

89. Due to the nature of the relationship between Defendants and Plaintiff and Class Members, Plaintiff and Class Members were entirely reliant upon Defendants to ensure that their PII/PHI was adequately protected. Plaintiff and Class Members had no way of verifying

or influencing the nature and extent of Defendants' or its vendors data security policies and practices, and Defendants was in an exclusive position to guard against the Data Breach.

90. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class Members' PII/PHI that they collected.

91. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI, which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

92. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

93. Plaintiff brings this claim on behalf of the nationwide class or, alternatively, on behalf of the California class based upon the laws of that state.

94. In connection with receiving healthcare services, Plaintiff and all other Class Members entered into implied contracts with Defendant.

95. Pursuant to these implied contracts, Plaintiff and Class Members paid money to Defendant, directly or through their insurance, and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiff and Class Members understood that Defendants would: (1) provide services to Plaintiff and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII/PHI; and (3) protect Plaintiff's and Class Members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

96. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and Defendant, on the other hand. Indeed, as set forth *supra*, Defendants recognized the importance of data security and the privacy of its customers' PII/PHI. Had Plaintiff and Class Members known that Defendants would not adequately protect their PII/PHI, they would not have utilized Defendants' services.

97. Plaintiff and Class Members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid for healthcare or other services utilizing Defendants' service.

98. Defendants breached their obligations under their implied contracts with Plaintiff and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, including by ensuring companies with whom Defendants contract implement and maintain reasonable security measures to protect PII/PHI, and in failing to implement and maintain security protocols and procedures to protect

Plaintiff's and Class Members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

99. Defendants' breach of their obligations under their implied contracts with Plaintiff and Class Members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class Members have suffered from the Data Breach.

100. Plaintiff and all other Class Members were damaged by Defendants' breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

101. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

102. Plaintiff brings this claim on behalf of the nationwide class or, alternatively, on behalf of the California class based upon the laws of that state.

103. This claim is pleaded in the alternative to the breach of implied contract claim.

104. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of monies paid to Defendants to be used for healthcare services and for adequate data protection for their PII/PHI.

105. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class Members' PII/PHI, as this was used to facilitate Defendants' services and allowed Defendants to operate their business.

106. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

107. Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because they failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

108. Plaintiff and Class Members have no adequate remedy at law.

109. Defendants should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiff Thukral and the California Class)

110. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

111. This claim is brought on behalf of Plaintiff Thukral and the California Class.

112. The CCPA was enacted to protect consumers' sensitive information from collection and use by businesses without appropriate notice and consent.

113. Through the conduct complained of herein, Defendants violated the CCPA by subjecting Plaintiff's and California Class Members' PII/PHI to unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violation of its duties to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

114. In accordance with Cal. Civ. Code §1798.150(b), on August 1, 2024, prior to the filing of this Complaint, Plaintiff's counsel served Defendants with notice of their CCPA violations by certified mail, return receipt requested.

115. Plaintiff currently seeks only injunctive relief in the form of an order enjoining Defendants from continuing to violate the CCPA.

116. If Defendants fail to agree to rectify the violations detailed herein, Plaintiff will seek leave to amend this Complaint to seek actual, punitive, and statutory damages, restitution, and any other relief the Court deems proper as a result of Defendants' CCPA violation.

COUNT VII
VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.* ("CCRA")
(On Behalf of Plaintiff Thukral and the California Class)

117. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

118. This claim is brought on behalf of Plaintiff Thukral and the California Class.

119. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

120. By failing to implement reasonable measures to protect Plaintiff's and California Class Members' PII/PHI, Defendants violated Civil Code § 1798.81.5.

121. In addition, by failing to promptly notify Plaintiff Thukral and all affected California Class Members that their PII/PHI had been exposed, Defendants violated Civil Code § 1798.82.

122. As a direct or proximate result of Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiff and California Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

123. In addition, by violating Civil Code §§ 1798.81.5 and 1798.82, Defendants "may be enjoined" under Civil Code Section 1798.84(e).

124. Plaintiff seeks restitution, damages, injunctive relief, and all other relief available under this cause of action on behalf of the California Class.

COUNT VIII
VIOLATIONS OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56 *ET SEQ.*
(On Behalf of Plaintiff Thukral and the California Class)

125. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

126. This claim is brought on behalf of Plaintiff Thukral and the California Class.

127. Defendant is a "Contractor" as defined by Cal. Civ. Code § 56.05(d) and/or a "Provider of Health Care" as defined in Cal. Civ. Code § 56.06.

128. Plaintiff and California Class Members are "Patients" as defined by Cal. Civ. Code § 56.05(k).

129. Plaintiff's and Class Members' PII/ PHI that was the subject of the Data Breach included "Medical Information" as defined by Cal. Civ. Code § 56.05(j).

130. Defendants had a duty under §§ 56.06 and 56.101 of the CMIA to maintain, store, and dispose of Plaintiff's and California Class Members' Medical Information in a manner that preserved its confidentiality.

131. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential medical information. Defendants violated these statutory obligations.

132. In violation of California's Confidentiality of Medical Information Act ("CMIA"), Defendant disclosed Medical Information of Plaintiff and California Class Members without first obtaining authorization.

133. In violation of the CMIA, Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class Members in a manner that did not preserve the confidentiality of that Medical Information.

134. In violation of the CMIA, Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class Members.

135. In violation of the CMIA, Defendant's electronic health record systems or electronic medical record systems did not protect and preserve the integrity of Plaintiff's and Class Members' Medical Information.

136. In violation of the CMIA, Defendant negligently released confidential information and records of Plaintiff and Class Members.

137. In violation of the CMIA, Defendant negligently disclosed Medical Information of Plaintiff and Class Members.

138. In violation of the CMIA, Defendant knowingly and willfully obtained, disclosed, and/or used Medical Information of Plaintiff and Class Members.

139. Because Defendants maintained Plaintiff's and Class Members' medical information in California, on California-based servers, where it ultimately disclosed such information to third parties, the CMIA equally applies to the entire affected class. *See, e.g.*, *Doe v. Meta Platforms, Inc.*, 690 F.Supp.3d 1064, 1079 (N.D. Cal. 2023) (holding that another statute, CIPA, could apply to non-residents of California, because the conduct at issue occurred in California).

140. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56 *et seq*., Plaintiff and Class Members now face an increased risk of future harm.

141. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiff and Class Members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of $1,000 for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, nominal damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 7, 2024

Respectfully submitted,

ANDERSON & KARRENBERG

/s/ *Jared Scott*
Jared Scott
Jacob W. Nelsom
jscott@aklawfirm.com
jnelson@aklawfirm.com
50 West Broadway, Suit 600
Salt Lake City, UT 84101
Telephone: 801.534.1700
Facsimile: 801.364.7697

Andrew W. Ferich (*pro hac vice* to be filed)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

Attorneys for Plaintiff & the Proposed Classes